CLAIMS

What is claimed is:

1. A method for protecting a computer in an opened share mode, comprising:
(a) running a computer on a network in an opened share mode;
(b) monitoring attempts to access the computer by applications utilizing the network;
(c) determining whether the applications attempt to modify the computer; and
(d) executing a security event in response to any attempt to modify the computer.

2. The method as recited in claim 1, wherein the opened share mode allows other computers on the network to access data stored on the computer.

3. The method as recited in claim 1, wherein the opened share mode includes a virtual opened share mode.

4. The method as recited in claim 3, wherein the virtual opened share mode indicates to other computers of an ability to write to the computer.

5. The method as recited in claim 4, wherein the computer operates in the virtual opened share mode by modifying an application program interface.

6. The method as recited in claim 5, wherein the application program interface includes an operating system application program interface.

7. The method as recited in claim 5, wherein the application program interface includes a network application program interface.

8. The method as recited in claim 1, wherein the opened share mode indicates a file structure parameter and a name parameter.

9. The method as recited in claim 1, wherein the opened share mode indicates a plurality of parameters that are randomly selected to prevent detection.

10. The method as recited in claim 1, wherein the opened share mode applies to each of a plurality of networks of which the computer is a member.

11. The method as recited in claim 1, wherein the opened share mode applies only to a predetermined list of application programs executable on the computer.

12. The method as recited in claim 11, wherein the predetermined list is created manually.

13. The method as recited in claim 11, wherein the predetermined list is created automatically.

14. The method as recited in claim 1, wherein the computer is run on the network in a plurality of opened share modes.

15. The method as recited in claim 1, wherein any attempt to modify the computer is utilized in a heuristic analysis for identifying a coordinated attack on multiple computers.

16. The method as recited in claim 1, wherein attempts to modify the computer are tracked.

17. The method as recited in claim 1, wherein it is determined whether the applications attempt to write to memory in the computer, and the security

event is executed in response to any attempt to write to memory in the computer.

18. The method as recited in claim 1, wherein it is determined whether the applications attempt to copy a virus to memory in the computer, and the security event is executed in response to any attempt to copy the virus to memory in the computer.

19. The method as recited in claim 1, wherein the security event includes logging the computer off the network in response to any attempt to modify the computer.

20. The method as recited in claim 1, wherein the security event includes terminating the application attempting to modify the computer.

21. The method as recited in claim 1, wherein the security event includes deleting the application attempting to modify the computer.

22. The method as recited in claim 1, wherein the security event includes an alert transmitted via the network.

23. The method as recited in claim 22, wherein the alert includes information associated with the application attempting to modify the computer.

24. A computer program product for protecting a computer in an opened share mode, comprising:

(a) computer code for running a computer on a network in an opened share mode;

(b) computer code for monitoring attempts to access the computer by applications utilizing the network;

(c) computer code for determining whether the applications attempt to modify the computer; and

(d) computer code for executing a security event in response to any attempt to modify the computer.

25. The computer program product as recited in claim 24, wherein the network includes the Internet.

26. The computer program product as recited in claim 24, wherein the opened share mode allows other computers on the network to access data stored on the computer.

27. The computer program product as recited in claim 24, wherein the opened share mode includes a virtual opened share mode.

28. The computer program product as recited in claim 27, wherein the virtual opened share mode indicates to other computers of an ability to write to the computer.

29. The computer program product as recited in claim 28, wherein the computer operates in the virtual opened share mode by modifying an application program interface.

30. The computer program product as recited in claim 29, wherein the application program interface includes an operating system application program interface.

31. The computer program product as recited in claim 30, wherein the application program interface includes a network application program interface.

32. The computer program product as recited in claim 24, wherein the opened share mode indicates a file structure parameter and a name parameter.

33. The computer program product as recited in claim 24, wherein the opened share mode indicates a plurality of parameters that are randomly selected to prevent detection.

34. The computer program product as recited in claim 24, wherein the opened share mode applies to each of a plurality of networks of which the computer is a member.

35. The computer program product as recited in claim 24, wherein the opened share mode applies only to a predetermined list of application programs executable on the computer.

36. The computer program product as recited in claim 35, wherein the predetermined list is created manually.

37. The computer program product as recited in claim 35, wherein the predetermined list is created automatically.

38. The computer program product as recited in claim 24, wherein the computer is run on the network in a plurality of opened share modes.

39. The computer program product as recited in claim 24, wherein any attempt to modify the computer is utilized in a heuristic analysis for identifying a coordinated attack on multiple computers.

40. The computer program product as recited in claim 24, wherein attempts to modify the computer are tracked.

41. The computer program product as recited in claim 24, wherein it is determined whether the applications attempt to write to memory in the computer, and the security event is executed in response to any attempt to write to memory in the computer.

42. The computer program product as recited in claim 24, wherein it is determined whether the applications attempt to copy a virus to memory in the computer, and the security event is executed in response to any attempt to copy the virus to memory in the computer.

43. The computer program product as recited in claim 24, wherein the security event includes logging the computer off the network in response to any attempt to modify the computer.

44. The computer program product as recited in claim 24, wherein the security event includes terminating the application attempting to modify the computer.

45. The computer program product as recited in claim 24, wherein the security event includes deleting the application attempting to modify the computer.

46. The computer program product as recited in claim 24, wherein the security event includes an alert transmitted via the network.

47. The computer program product as recited in claim 46, wherein the alert includes information associated with the application attempting to modify the computer.

48. The computer program product as recited in claim 24, wherein at least a portion of the computer code resides on a gateway.

49. The computer program product as recited in claim 48, wherein the security event includes blocking access to the computer.

50. A system for protecting a computer in an opened share mode, comprising:
(a) logic for running a computer on a network in an opened share mode;
(b) logic for monitoring attempts to access the computer by applications utilizing the network;
(c) logic for determining whether the applications attempt to modify the computer; and
(d) logic for executing a security event in response to any attempt to modify the computer.

51. A method for protecting a computer in an opened share mode, comprising:
(a) running a computer on a network in a virtual opened share mode, wherein the virtual opened share mode allows other computers on the network to access predetermined data and programs resident on the computer, and indicates to other computers of an ability to write to the computer;
(b) monitoring attempts to access the computer by applications utilizing the network;
(c) determining whether the applications attempt to modify the computer;
(d) tracking the attempts of the applications to modify the computers;
(e) transmitting an alert via the network in response to any attempt to modify the computer, wherein the alert includes information associated with the applications attempting to modify the computer;
(f) logging the computer off the network in response to any attempt to modify the computer; and
(g) deleting any application attempting to modify the computer;
(h) wherein any attempt to modify the computer is utilized in a heuristic analysis for identifying a coordinated attack on multiple computers.

52. A computer program product for protecting a computer in an opened share mode, comprising:

(a) computer code for running a computer on a network in a virtual opened share mode, wherein the virtual opened share mode allows other computers on the network to access predetermined data and programs resident on the computer, and indicates to other computers of an ability to write to the computer;

(b) computer code for monitoring attempts to access the computer by applications utilizing the network;

(c) computer code for determining whether the applications attempt to modify the computer;

(d) computer code for tracking the attempts of the applications to modify the computers;

(e) computer code for transmitting an alert via the network in response to any attempt to modify the computer, wherein the alert includes information associated with the applications attempting to modify the computer;

(f) computer code for logging the computer off the network in response to any attempt to modify the computer; and

(g) computer code for deleting any application attempting to modify the computer;

(h) wherein any attempt to modify the computer is utilized in a heuristic analysis for identifying a coordinated attack on multiple computers.